Failles découvertes dans eMule et dans Winamp

Deux failles, pour deux produits phares… Avec eDonkey, eMule est l'une des plate-formes de 'peer-to-peer' (échange gratuit de fichiers) les plus utilisées dans le monde notamment pour les films, les applications… Bref, c'est l'outil quasi idéal pour l'internaute téléchargeur.

Mais le programme, qui est en open-source, peut se révéler dangereux. Les spécialistes du site K-Otik nous apprennent qu'une faille a été découverte dans la plate-forme. Elle permet à un pirate de prendre le contrôle à distance de la machine de l'utilisateur. *« Cette faille de type « stack overflow » se situe au niveau de la fonction DecodeBase16 qui décode des valeurs sans vérification de leur longueur. Cette fonction vulnérable est utilisée cinq fois dans le code (trois fois dans le serveur web qui nécessite une authentification, et deux fois dans le client IRC) »*, décrit K-Otik. Ce sont donc des fonctions « serveurs » et « chat » du programme qui sont concernées. Conséquence: les utilisateurs qui n'ont pas de serveur Web ne pourront pas être victimes de cette faille. Idem pour ceux qui n'utilisent pas la fonction « chat ». Toutes les versions d'eMule sont concernées par ce trou. Seule la dernière version (0.42e) contient le correctif. Il suffit de la télécharger sur le site d'eMule. Nos confrères de K-Otik nous révèlent également l'existence d'une faille dans le très populaire lecteur audio Winamp: *« Elle pourrait être exploitée par un attaquant distant afin de compromettre un système vulnérable »*. *« Cette faille de type*heap overflow*est causée par une erreur présente dans « in_mod.dll » qui ne gère pas correctement certains fichiers media « .xm » (Fasttracker 2Fce qui pourrait être exploité par un attaquant distant afin d'exécuter des commandes arbitraires sur une machine vulnérable en incitant un utilisateur à visiter un site malicieux) »*, explique le site. Les versions 2.91 à 5.02 sont touchées. Pour se protéger, les utilisateurs sont invités à télécharger la version 5.03 du lecteur. Le site de K-Otik.